DEPARTMENT OF THE NAVY
BUREAU OF NAVAL PERSONNEL
5720 INTEGRITY DRIVE
MILLINGTON TN 38055-0000

IN REPLY REFER TO
BUPERSINST 5239.1B
PERS-014
5 Apr 2001

BUPERS INSTRUCTION 5239.1B

From: Chief of Naval Personnel

Subj: BUREAU OF NAVAL PERSONNEL (BUPERS) INFORMATION SYSTEMS SECURITY (INFOSEC) PROGRAM

Ref: (a) Computer Security Act of 1987 (Public Law 100-235)
(b) OMB Circular No. A-130 of 8 Feb 96
(c) DODD 5200.28 of 21 Mar 88
(d) SECNAVINST 5239.3
(e) OPNAVINST 5239.1B
(f) SECNAVINST 5000.2B
(g) SECNAVINST 5510.36
(h) DOD 5500.7-R, of Aug 93
(i) DODI 5200.40 of 30 Dec 97
(j) SECNAVINST 5214.2B
(k) SECNAVINST 5720.44A
(l) OPNAVINST C5510.93 (NOTAL)

Encl: (1) AIS Security Procedures and Policies
(2) BUPERS Activity Information Systems Security Plan (ISSP)
(3) NAVPERS 5239/3 (Rev 2-98), BUPERS LAN External Communications Access Request,
(4) INFOSEC Training Outline
(5) INFOSEC Warning Screen
(6) NAVPERS 5239/1 (Rev 2-98), BUPERS Automated Information System (AIS) Security Incident Report
(7) NAVPERS 5239/4(Rev 4-99), PERSNET LAN Account Request
(8) NAVPERS 5239/5 (12-00), Personally-owned Computer Hardware/Software User Agreement
(9) NAVPERS 5239/6 (01-01), Secret Internet Protocol Router Network (SIPRNET) LAN Account Request

1. Purpose. To provide comprehensive command security policy and to establish and implement an INFOSEC program to meet requirements of references (a) through (l). This instruction has been revised substantially and should be reviewed in its entirety.

2. Cancellation. BUPERSINST 5239.1A.

3. Background. References (a) through (i) direct each agency to implement and maintain an Automated Information Systems (AIS) security program to assure that adequate security is provided for all information collected, processed, transmitted, stored, or disseminated in general support systems and major applications. Former BUPERS directives for AIS systems did not include guidance for protection of Local Area Networks (LANs) or Wide Area Networks (WANs). With technological advancements in communications has come increased danger of losing sensitive data and ultimately crippling our organization through vulnerabilities in these systems. This policy is designed to bring these vulnerabilities to a level of risk that will protect our resources without unduly impeding production. All sensitive but unclassified systems must be safeguarded so that such information is only accessed by authorized persons, is used only for its intended purpose, retains its content integrity, and is marked properly as required. As stated in Information Assurance (IA) Pub-5239-15, the nature of the Department of the Navy (DON) mission, accompanied by connectivity and data aggregation issues, has led to the determination that all DON unclassified systems are sensitive.

4. Scope. Chief of Naval Personnel (CHNAVPERS) is responsible for ensuring compliance with the DON INFOSEC program identified in references (d) and (e).

5. Policy. Ultimate responsibility for security of BUPERS information systems and data rests with the Designated Approving Authority (DAA). Organizational heads are responsible for ensuring their employees comply with this policy and use the Internet for official government business and other authorized purposes only. Individual users will be held accountable for their use and Internet access. Unless access to an external or internal function or system is specifically allowed, the function or system access is not allowed. Allowing only the minimum set of accesses ensures that if users make mistakes, or if intruders succeed in masquerading as legitimate users, the scope of the potential damage is limited. Enclosure (1) provides additional AIS security procedures and policies.

a. Violations of this instruction include, but are not limited to use of Internet/E-Mail for other than official business or other authorized purposes and possession or use of games or other entertainment software on a government workstation. Infractions will be charged under the Manual for Courts-Martial (MCM) for military personnel. Remedies for disciplinary action against civilian employees who are in violation could be reprimand, suspension, or removal depending on mitigating or aggravating factors. The appropriate contract delivery order "Standards Enforcement" sections applies for contractor personnel.

b. Copyright and Licensing. Purchased/licensed software will be used per vendor's established copyright/license provisions. Command personnel may be held liable for any infringement of copyrighted software licensing agreements per IA Pub-5239-29.

c. Monitoring. Only security-appointed personnel, Information Systems Security Manager (ISSM), Information System Security Officers (ISSOs), Network Security Officers (NSOs), and system administrators are authorized to monitor AISs. Monitoring will be conducted per IA Pub-5239-08 and to the extent necessary to ensure that only official government business and other authorized purposes are conducted.

6. Responsibilities

a. Commanders/Commanding Officers (COs)/Officers-in-Charge (OICs). The commander/CO/OIC is the DAA. DAA is the official with authority to accredit all AIS for which they are the DAA and grant Interim Authority to Operate (IATO) for all systems not accredited and in addition is responsible for

(1) ensuring the development of an INFOSEC program to provide adequate security to protect all AIS and ensure compliance with the DON Security program.

(2) appointing an ISSM in writing to act as the focal point for all INFOSEC matters.

(3) ensuring that contract specifications for AIS equipment, software, maintenance and professional service satisfy the INFOSEC requirements.

(4) ensuring that security requirements are included in Life Cycle Management (LCM) documentation as required in reference (d). Security will be built into the system whenever possible, to relieve the users of assessing and developing security for the system.

b. ISSM. The ISSM will perform their duties as delineated in IA Pub-5239-04 and as indicated below.

(1) Coordinate with the command security manager on matters concerning INFOSEC to comply with references (d), (e) and (g).

(2) Ensure that an Information Systems Security Plan (ISSP) and accreditation schedule are developed and maintained.

(3) Ensure that ISSO and Terminal Area Security Officers (TASO) are appointed in writing where applicable.

(4) Ensure accreditation support documentation is developed and maintained including Risk Assessment, Security Test & Evaluation (ST&E), and a contingency plan.

(5) Ensure applicable Security Operating Procedures (SOPs) are established for all departments and divisions.

(6) Coordinate requests for Transient Electro-Magnetic Pulse Emanation Standard (TEMPEST) surveys and zoning per reference (m).

(7) Ensure all security incidents or violations are investigated, documented, and reported to proper authority (i.e., command security manager; CO/OIC; Commander, Naval Computer Telecommunications Command (COMNAVCOMTELCOM); etc.).

(8) Conduct periodic checks to ensure INFOSEC requirements are met. As a minimum, checks will be performed annually or when the command's security posture changes.

(9) Ensure configuration management of all command hardware and software.

(10) Ensure all users are given annual INFOSEC training.

(11) Monitor AIS procurements for security impact to ensure compliance with security requirements.

c. ISSO. Each department or division will appoint an ISSO. ISSO will perform their duties per IA Pub-5239-07 and as indicated below.

(1) Coordinate with the ISSM all actions on matters concerning INFOSEC.

(2) Ensure that personnel security procedures are developed and implemented.

(3) Ensure that all INFOSEC incidents or violations are properly investigated, documented, and reported to the ISSM.

(4) Monitor system activity by conducting periodic checks to ensure command security policies and procedures are followed.

(5) Develop and submit an ISSP for each major application and general support system under their cognizance to the ISSM. Guidance for developing an ISSP is provided in enclosure (2). The ISSP will be included with the certification and accreditation process.

d. NSO. The sponsoring Directorate of each network will appoint the NSO in writing. The NSO will perform their duties per IA Pub-5239-08 and as indicated below.

(1) Ensure that countermeasures and security requirements are implemented for each node of the network. Ensure a Memorandum of Agreement (MOA)/Memorandum of Understanding (MOU) for security is established with each node/terminal located in another activity and implemented before the node/terminal is connected to the network.

(2) Ensure and promulgate the standard security procedures governing network operations.

(3) Ensure that security measures and procedures used at network nodes fully support the security integrity of the network.

(4) Maintain liaison with the ISSM and all ISSOs and TASOs in the network.

e. TASO. The cognizant officer for each remote site that has a terminal connection to a network will designate a TASO in writing. TASO is the representative of the ISSO in matters pertaining to security of each terminal. TASO will enforce applicable security requirements implemented by the ISSM in the Standard Operating Instruction.

f. Users. All AIS users and their responsible supervisors will familiarize themselves with the contents of this instruction. All users will ensure the following procedures are strictly adhered to:

(1) Each user will turn off their computer prior to securing for the day.

(2) No user will leave a terminal logged onto the network while away from their workstation.

(3) No user will gain access on a terminal by other than their own login identification.

(4) All users are responsible for guarding their password and ensuring that it is not divulged to anyone.

(5) No user will attempt to perform any function for which they are not authorized or trained to perform.

(6) In the event of a compromise or password failure, the user must notify their ISSO or the ISSM immediately in order that appropriate and timely action may be taken.

(7) Supervisors will notify their ISSO or the ISSM when subordinates are disqualified as authorized users due to transfer, termination, job change, or other cause.

7. Action. BUPERS, BUPERS claimant activities, BUPERS sponsored contractors, and activities located at the Navy Annex (FOB #2) will adhere to the policies and procedures in this instruction.

8. Report and Forms

a. Report. Reference (j) exempts reporting requirement(s) contained in paragraph 5p from reports control.

b. Forms. The following forms may be reproduced locally or can be obtained from the BUPERS ISSM:

(1) NAVPERS 5239/1 (Rev 2-98), BUPERS AIS Security Incident Report.

(2) NAVPERS 5239/3 (Rev 2-98), BUPERS LAN External Communications Access Request.

(3) NAVPERS 5239/4 (Rev 4-99), PERSNET LAN Account Request.

(4) NAVPERS 5239/5 (Rev. 12-00), Personally-owned Personal Digital Assistant (PDA) User Agreement.

(5) NAVPERS 5239/6 (01-01) Secret Internet Protocol Router Network (SIPRNET) LAN Account Request.

G. L. HOEWING
Rear Admiral, U.S. Navy
Deputy Chief of Naval Personnel

Distribution:
SNDL A3 (CNO)(N1T, N10, N12, and N13 only)
FJA (Shore Activities under the Command of CHNAVPERS)
FJB1 (COMNAVCRUITCOM)
BUPERSINST 5218.3E
1A Chief, Special Assistants, Staff Office Directors, and Assistant Chiefs
1B Division Directors, Staff Office Directors, and Special Assistants to ACNPs
2A Branch/Staff Office Heads, and Special Assistants to Division Directors

Copy to:
SNDL C55A (DAPMA San Diego and Norfolk)
C55F (NAMALA)

AIS SECURITY PROCEDURES AND POLICIES

1. Access Warning. The INFOSEC Warning Screen, enclosure (5), must be displayed on all computer systems (network or stand-alone) prior to a successful login. The warning screen will include a statement that the use of Department of Defense (DOD) computer system constitutes consent to monitoring at all times. It will also state that if unauthorized activity is identified, the user is subject to disciplinary action.

2. LAN Access. Prior to connection to BUPERS LAN all users must submit a PERSNET LAN Account Request, enclosure (7), to their ISSO.

3. Passwords. Passwords should not be in the dictionary, should not be any permutation of one's name, and should not be a birth date. Passwords must be a minimum of eight or a maximum of fifteen characters in length; not representing words, names, or phrases; and must contain a combination of letters, numbers, and special characters, such as the "&" sign. Users are not to share passwords nor keep passwords in unsecured locations, such as on written notes, hard disk storage lists, or script files. The host communications network will allow three attempts to enter correct identification and password. Following three failed attempts, the host communications network will terminate connection and lock the user out of the system. Passwords must be changed every 3 months.

4. Electronic Mail (E-Mail). E-Mail will be used only for official business or other authorized purposes. E-Mail will be routed through main communication server firewalls, e.g., gateway, bridge, router, or brouter, to detect and prevent unauthorized events, including but not limited to hacking, unauthorized access, technological attacks, virus attacks, impersonation, network penetration, destruction of information, and browsing. Sensitive unclassified information shall only be sent to authorized recipients.

a. Command personnel are responsible for considering the effect of data aggregation when determining sensitivity of information. Some elements, when considered separately, may be of relatively low sensitivity; however, when considered collectively, these same elements become more sensitive to unauthorized disclosure/modification. These effects of the

information will be considered before transmission of E-Mail. Command personnel are responsible for ensuring that appropriate labels and statements are applied (i.e., Privacy Act, For Official Use Only, etc.) prior to transmission. Detailed guidance on proper use of labels and statements can be obtained via the command ISSM.

b. Copies of E-Mail transmissions are subject to possible release under the Freedom of Information Act (FOIA) and discovery in litigation. They are also subject to records retention requirements of the Federal Records Act.

c. E-Mail system is not to be used for unprofessional or derogatory personal remarks that are directed toward an individual or groups of individuals. Transmission of pornographic or sexually explicit materials or materials containing profane or unprofessional language, questionable humor, or for sexual harassment is strictly prohibited. E-Mail should be treated as an "official" work product. E-Mail frequently receives a wider distribution and may be kept longer than the author intends. Communication with an associate that may be reasonable in a phone call or personal conversation may not be reasonable to commit to writing either electronically or in hard copy form. E-Mail should not be used to conduct an argument or to make comments that could be considered less than professional.

d. E-Mail system is not to be used for chain letters or advertisement of private or social interests, or distribution of jokes or games. Any chain letter or advertisement received should not be forwarded, and should be deleted upon receipt.

e. Any infractions of the E-Mail system will be immediately reported to the ISSO.

f. Only authorized individuals have the use of address groups, such as “All LAN Users,” created to broadcast and distribute mail to command-wide, global, or other external addresses. All other users who require mail broadcasting must receive written permission from their division director or deputy director. In their absence, written permission must be obtained from the code-designated ISSO. Management and use of address groups created to disseminate information within an office, unit, section, branch, division, or department is the

responsibility of the specific office, unit, section, branch, division, or department.

5. Internet Web Browsing. Internet usage will be for official government business or other authorized purposes only. Users will not access Internet Web sites whose contents might be considered pornographic. Users are prohibited from downloading/displaying any material that is considered pornographic or offensive in nature, including all audio and visual material. Users will not access or download from Internet Web sites with content that may promote racism, bigotry, or anti-semitism. Users will not conduct or promote private business enterprises from government systems.

a. BUPERS provides authorized users with access to unclassified public networks for the sole purpose of communication that is directly related to official unclassified government business and other authorized purposes. Any violation of the following can result in disciplinary or administrative action. Per reference (h) permissible use of the Internet enhances the users' professional skills and thus serves a legitimate public interest. Permissible uses are defined to include all uses not prohibited by law, regulation, instruction, or command policy. Permissible uses indicated by reference (h) generally require supervisor’s permission. Prohibited uses include

(1) introducing classified information into an unclassified system or environment.

(2) accessing, storing, processing, displaying, distributing, transmitting, or viewing material that is pornographic, racist, promotive of hate crimes, or subversive in nature.

(3) storing, accessing, processing, or distributing classified, proprietary, sensitive, "For Official Use Only" (FOUO), or Privacy Act protected information in violation of established security and information release policies.

(4) obtaining, installing, copying, pasting, transferring, or using software or other materials obtained in violation of the appropriate vendor's patent, copyright, trade secret, or license agreement.

(5) knowingly writing, coding, compiling, storing, transmitting, or transferring malicious software codes, to include viruses, logic bombs, worms, and macro viruses.

(6) promoting partisan political activity.

(7) disseminating religious materials outside an established command religious program.

(8) using the system for personal financial gain, such as advertising or soliciting services or sale of personal property, with the exception of using a command-approved mechanism, such as a welfare and recreation electronic bulletin board for advertising personal items for sale.

(9) fund raising activities, either for profit or non-profit, unless the activity is specifically approved by the command (e.g., welfare and recreation car washes).

(10) gambling, wagering, or placing of any bets.

(11) writing, forwarding, or participating in chain letters.

(12) posting personal home pages.

(13) personal encryption of electronic communications is strictly prohibited.

6. Games. Use of entertainment or game software, regardless of origin, is prohibited. ISSOs shall ensure that such software is not loaded on any information system under their cognizance.

7. INFOSEC Awareness and Training. Reference (e) requires annual mandatory training in computer security awareness and accepted computer security practices for all personnel having access to computer information systems to include contractors. ISSM will provide guidance to ISSOs for the INFOSEC Training Program, which will include an annual awareness training class. In-house training can be provided through films, computer base training, oral classroom presentations, or videos. Methods used will depend on the depth of training required for particular

information systems areas and duties of users to be trained. Enclosure (4) is a guide for developing a Security Training Program.

8. Malicious Code. It will be considered a major security violation for any user (civilian, military, or contractor) to deliberately introduce malicious codes (computer program codes written with intent to cause harm or destruction that is inserted into a valid computer program) or computer viruses into the command's information systems. It is also a security violation to withhold information necessary for effective implementation of countermeasures or anti-virus procedures. All personal computers (PCs) and networks must have an activated anti-virus software program installed; it must not be removed or disabled from the system.

9. Virus. Users must be aware of the following signs of computer virus infections and the necessary action to take if a virus is suspected:

a. AIS operates at a slower processing speed than normal.

b. AIS shows unexplained reduction of storage capacity.

c. Data shows unexplained extensions or files.

d. Unexplained AIS crashes.

e. There are many programs with the same date/time in their last update field.

f. If a virus problem is detected, take the following action:

(1) STOP! DO NOT USE THE PC; DO NOT TURN OFF THE PC.

(2) Notify your supervisor, then your ISSO. If ISSO cannot be reached, notify ISSM immediately.

(3) If applicable, collect all storage media from others who share your diskettes.

(4) ISSO will run virus detection software to identify and isolate the attack. ISSO will clean and disinfect the

system and forward incident reports to the ISSM. Users must scan diskettes to ensure diskettes are virus free. If viruses are found they are to be reported to the ISSO.

10. Security Incident Reporting. A security incident is an attempt to exploit DON information systems or networks. Security incidents include penetration of computer systems, exploitation of technical and administrative vulnerabilities, introduction of computer viruses or other forms of malicious code, and theft or destruction of hardware, software, or data. These types of attacks can result in compromise of information, denial of service, and other related disruptions that can severely impact the command's mission and functions. Users must report all security incidents to their ISSO. The ISSO will complete and forward enclosure (6) within 24 hours of the reported incident to the ISSM. ISSM will notify DAA and investigate the report to determine if Naval Computer Incident Response Team (NAVCIRT) at Fleet Information Warfare Center (FIWC) needs to be notified.

11. Personnel/Physical Security. All individuals shall be screened to ensure a level of trustworthiness commensurate with their duties. Physical security measures will be taken to safeguard personnel and to prevent unauthorized access to equipment, installations, material, computer media, and documents. In addition, safeguards will be provided against espionage, sabotage, damage, and theft.

12. Systems Planning and Design. Information systems planning and design activities shall have adequate internal controls. Per reference (c), reasonable assurance must be provided to ensure recording, processing, and reporting of data are properly performed during operation of the information systems. Project managers shall comply with the Life Cycle Management (LCM) policies and approval requirements for the information systems security in reference (f).

13. Physical Security of Information Systems (IS) Equipment. All IS equipment must be physically protected to prevent theft. Command inventory management and physical security will be notified of all IS equipment reported missing, lost, stolen, or recovered.

14. Removal of IS Equipment. Removal of IS equipment (including laptops) must be approved by user's ISSO and will be accompanied by a property pass. Users will be held responsible for safeguarding and physical security of equipment and information while it is out of the command's control.

15. External Connections. There must be written approval from ISSM for all systems (including remote systems) using non-dial up connectivity. IS with servers (including Web Servers) which are connected to unclassified publicly accessible computer networks (i.e., Internet, etc.) will employ appropriate safeguards (i.e., firewalls, encryption, etc.) as necessary to ensure the command's integrity, authenticity, privacy, and availability of information systems.

16. Non-Government or personally-owned Computer Hardware or Software

a. Under no circumstance will there be classified information processed on a non-government or personally owned computer.

b. Use of non-government, personally owned computer hardware and software is prohibited; however, if an urgent validated requirement exists to accomplish an official job and the hardware/software is not currently available, a user may request authorization for use of personally owned hardware or software. User must submit a written request and enclosure (8) via their ISSO and division director for use of this hardware or software. (It should be noted that user preference is not criteria for the use of non-government, personally owned hardware or software.)

c. The use of unauthorized computer hardware or software without permission is strictly prohibited. Unauthorized hardware or software found on a BUPERS PC must be reported to the user's division director and the ISSM. The designated ISSO will request the user remove the unauthorized hardware or software. If user does not remove the hardware or software, the ISSO will remove the unauthorized hardware or software and report the user to their division director and ISSM for possible disciplinary action.

d. If circumstances are that time does not allow for the procurement of hardware or software, the user may be authorized the use of personally owned hardware/software only until it is made available. The following details the process for use of personally owned hardware or software:

(1) The user's written request and enclosure (8) must be approved by the ISSM prior to bringing hardware/software on-site for use on a government-owned computer. When the hardware or software is brought on-site, the user will turn it over to their ISSO along with the original license and software (compact or floppy disks).

(2) The ISSO will submit enclosure (8) and the original software and license agreements to the system administrator for compatibility testing to ensure there is no measurable impact on network operations or PC/network support. If it is determined there is an impact the user may be required to use subject software in a stand-alone environment.

(3) The ISSO will ensure the installation of all software and maintain the original copy of ownership documents and floppy or compact disks for the entire period in which the hardware/software is in use within the command.

(4) The ISSO will return all hardware or software and associated ownership documents to the user when the command has received government-owned hardware or software, the completion of the project, or the user requests the return of hardware or software for removal from the command.

e. BUPERS will not be responsible for support of non-government, personally owned software and will not be liable for lost, damaged, or stolen personally owned hardware or software.

f. Non-government owned and government owned hardware/software will only be installed by authorized personnel, ISSO, Local Area Network (LAN) personnel, or PC support technicians.

g. Use of non-government owned hardware or software will be limited to single user machine for which approval was granted. Under no circumstances will copyright laws be violated, or single licensed user software be installed on multiple machines.

17. Dial-In/Dial-Out. Banks of modems and communications servers have been installed on the BUPERS LAN to support dial-in/dial-out access. NO DESKTOP MODEMS ARE AUTHORIZED ON AN AIS CONNECTED TO BUPERS LAN. No modems will be connected directly to the BUPERS LAN. Stand-alone modems and modems connected to Office Automation Networks (OANs) will be allowed if authorized by the DAA via memorandum with endorsement by the ISSM. As required by reference (d), all connections will display the INFOSEC warning screen, enclosure (5), before proper login. It is the responsibility of the ISSO to ensure anti-virus protection software is installed and activated on any AIS with dial-in/dial-out and Internet access.

a. Dial-In Access. Primary means of dial-in access will be via BUPERS LAN modem pool. No other modem will be connected directly to the BUPERS LAN without prior approval. To request exemption from this policy, a written justification signed by the requesting director and ISSO is required to be submitted to ISSM for approval. The dial-in/dial-out host network manager will maintain an access list of authorized dial-in users. To obtain dial-in/dial-out access, a user must submit BUPERS LAN External Communications Access Request, enclosure (3), for approval by the NSO. Upon establishing a connection, the host communications device must authenticate login identification and password. For remote node access, host will be configured to allow users three attempts to enter server name, login identification, and password before terminating connection and rebooting. Remote users will be denied access to host or other non-server-based resources under all circumstances. Users must be locked in a circular login pattern to prevent scanning for available file servers. NOTE: This will help to ensure users know the name of the destination server. Where the need for dial-in access exceeds the capability of the BUPERS LAN, access may be granted through modem pools on stand-alone OANs. Stand-alone modems will not be permitted for any personal computer connected to any BUPERS LAN or OAN. Software used to support dial-in must provide for the capability to audit user's

login identification, time and duration of session. BUPERS network or an Integrated Services Digital Network (ISDN) communications server must support a modem pool.

18. Marking/Handling

a. Data. All human-readable output must be marked to the highest classification. If the AIS does not have the capability of marking the output, then this must be accomplished manually. Automated markings are not considered reliable unless the AIS meets B1 security certification.

b. Magnetic Media

(1) Color coded labels/disks per reference (g) will be used to distinguish classification of all media.

(2) Classified media will be handled, stored, and controlled per reference (g).

(3) Removable media that can be secured is encouraged for classified systems. Fixed, internal hard disks should be avoided for classified processing; however, if removable media cannot be used, ensure proper physical and personnel security guidelines are implemented to the level of data being processed.

(4) Releasing Media to Unsecured Area. The DAA is responsible for ensuring the proper procedures are in place for magnetic media removal. When multiple levels of classified materials are processed, the activity DAA is responsible for ensuring inadvertent disclosure does not occur. If classified media must be removed, then the proper procedures shall be followed in IA Pub-5239-26. Repair contractors should be cleared, the activity must ensure that media being used by the contractor is copyrighted, and that government files are not downloaded and removed from command.

(5) Degaussing/Clearing. Following are current procedures:

(a) Sensitive Unclassified. Media, which has been used from sensitive unclassified information, will be formatted and erased before released/reused.

(b) Downgrading. Classified floppy disks and magnetic hard disks can be degaussed with an approved degausser. Approved degaussers appear on the evaluated product list in the Information Systems Security Products and Service Catalog. In addition, classified hard disks can be downgraded by the overwrite procedures outlined in IA Pub-5239-26.

(c) Unusable Disks. Disks that have been rendered unusable must be destroyed. When an approved degausser is not available, floppy disks may be cut in half and placed in a burn bag. To purge hard drives follow procedures outlined in IA Pub-5239-26.

19. Public Disclosure. Prior to public disclosure of limitation, vulnerabilities, or capabilities, AISs must be in compliance with references (g) and (k).

20. Emanations Security. All AIS's must be per TEMPEST guidance provided in reference (l).

21. Secret Internet Protocol Router Network (SIPRNET). Command personnel requesting access to SIPRNET must have the proper clearance, need-to-know, and access to Secret information granted by the command security manager. Once access has been granted the individual must submit enclosure (9) for SIPRNET access. All personnel having access to SIPRNET will maintain control of the classified information per reference (g).

BUREAU OF NAVAL PERSONNEL
ACTIVITY INFORMATION SYSTEMS SECURITY PLAN (ISSP)

1. System/Unit Identification. Enter complete title and mailing address of the organization or the activity for which the information system accreditation is being requested.

Example:
Bureau of Naval Personnel (BUPERS)
5720 Integrity Drive
BLDG 769 (PERS-014)
Millington, TN 38055-0140

2. Support Personnel

a. ISSM and ISSO. Enter name (with rank), title, organization/office symbol, telephone numbers, and Defense Message System (DMS)/Automated Digital Network (AUTODIN) address of the ISSM and ISSO responsible for the information system(s) documented in this package.

b. System Administrator (SA). Enter name (with rank), title, organization/office symbol, telephone numbers, and DMS/AUTODIN address of the SA responsible for the information system(s) documented in this plan.

3. Mission Description

a. Mission and Criticality of the Information System(s). Describe role of the information system(s) documented in this plan in support of the organization's mission. Include a description of any network connectivity requirements. A statement should be included that discusses the criticality of the system(s) to the accomplishment of the mission. This criticality statement should also assess the importance of the system(s) to other DON commands and organizations being able to also successfully accomplish their missions. If the requester is a contractor, enter the contract number, contract period, project identification, and the government office responsible for monitoring the contract.

b. Identification of the Accreditor, System(s) Ownership.

c. Data Sensitivity. Estimate in percentage the amount of information anticipated to be processed on the information system(s) by the following classification:

(1) Unclassified.

(2) Sensitive but Unclassified

(3) Confidential.

(4) Secret.

(5) Top Secret.

State types of data processed on the system(s) such as Privacy Act, proprietary, procurement sensitive, others.

d. Identity of System(s) Users. State the formal clearance, formal access, and need-to-know requirements of all users, both direct and indirect, which are anticipated to be authorized access to the information system(s). State the types of established accounts and users on the AISs. Identify the number of users by type to include: Super (Privileged), Root, Local, Remote, Second Party, Contractors, Maintenance, and others not identified by these categories.

e. Mode of Operation. State the information system’s security mode of operation (Dedicated, System High, Compartmented (Partitioned), or Multi-level), and whether the system is attended, unattended, or remotely controlled while operating.

f. Functional Description/Requirements.

4. Threat Analysis

a. Environment. State the information system's operating location, type of facility (fixed, tactical, or both), and if tactical whether ground-mobile, airborne, or afloat. State the system's usage to include its general usage (mission or mission support), connectivity (STAND-ALONE, local connectivity, external communications, or combinations of connectivity).

b. Threat Summary. Chief of Naval Operations (CNO) (N6) INFOSEC staff, FIWC and other organizations shall provide updated threat information specifically for DON information systems environments. Threat information shall be analyzed by the organization preparing the ISSP, and an assessment made of the applicability of the various types of threats to the specific information system(s) being discussed in the ISSP. The ISSM and ISSO at a site shall play a lead role in performing this assessment.

c. Risk Assessment Summary. Risk assessment identifies the threats, vulnerabilities, and risks to a network. Although there are a variety of risk assessment packages and methodologies currently being used in DON, the preferred risk assessment methodology recommended for use in DON is contained in IA Pub-5239-16, the "Risk Assessment Guidebook." DON-sponsored/funded training courses will teach the risk assessment process contained in IA Pub-5239-16. It presents a methodology for conducting a risk assessment using one of four types: survey, basic, intermediate, and full risk assessment; and has direct applicability to today's distributed networking environment. The Trusted Risk Assessment Methodology (TRAM), which has been used for several years in DON, is primarily intended for stand-alone computers. TRAM may not be useful in today's environment in which network security connection approval requirements of networks owned by joint activities and agencies (such as Defense Information Systems Agency (DISA)), mandate modern, updated processes. For the implementation of the classified and Military Locator System (MLS) portions of DMS within DON, scheduled for the latter part of this decade, the risk assessment process provided in the IA Pub-5239-16 has direct applicability.

5. Architectural Description

a. Hardware. List all hardware components installed and operating on the system(s) in this package. Include all communication and encryption devices supporting network connectivity.

b. Software. List all software installed and operating on the system(s). Include all operating systems, database management systems, communications software, security software, off-the-shelf software, etc.

c. Accreditation Boundary. Describe the system's architecture, including physical location of system's components, wiring diagrams, floor layout.

d. External Connections. List all network connectivity being performed by the system(s) in this package. For each connection enter the following: types of services or applications (E-Mail, file transfer, remote query, remote access, etc.).

6. System(s) Security Requirements

a. Security Policy Statement.

b. Security Requirements.

c. Summary of Administrative, Technical, and Operational Security Features. Discuss the security features implemented in the system(s). Terms to be covered include (as applicable or as directed by the DAA system administrators guide), user acknowledgment forms, warning/monitoring banner, discretionary access controls, audit trails, password management, configuration management, contingency plans, back-up procedures, emergency destruction, security education, security features users guide, guards, firewalls, etc.

d. Concept of Operations.

7. Certification

a. Security Test & Evaluation (ST&E). ST&E documentation should also be part of the accreditation package. ST&E plans and procedures identify each of the countermeasures to be tested and the method used to determine the effectiveness of the countermeasures. ST&E checklists can be used to evaluate the effectiveness of countermeasures implemented on an AIS or network system. The checklist approach may be appropriate when a full-blown ST&E is deemed necessary by the DAA, as determined by the flexibility of the AIS and the level of risk. The checklists help ensure that the AIS or network is operating within an acceptable level of risk. The ST&E report documents the execution and results of the ST&E plan/procedures. It analyzes the findings of the ST&E plan/procedures and lists the recommendations to correct any identified deficiencies. IA

Pub-5239-18 provides information on how to perform a ST&E for AISs, embedded computers, and networks. It addresses microcomputers, minicomputers, mainframes, and specialized computers in both STAND-ALONE and networked environments. The guidebook provides guidance and procedures to security managers and users for conducting ST&Es.

b. Copy of Completed "BUPERS AIS and Network Security Inspection Checklist."

c. Summary of Type II Certification Effort (if applicable). Provide copies of key documents or test results as enclosures to the Certification and Accreditation (C&A).

d. Statement of Security Concerns. Description of how systems satisfy security requirements. Describe the most significant security concerns for this particular system (e.g., unauthorized users may gain access to the system or data, data corruption, system availability, security incidents, etc.). Provide copies of any MOAs.

e. Recommendation. ISSM provides residual risk statement, including rationale for why residual risks should be accepted/rejected and recommends approval or non-approval to operate the system(s).

8. Accreditation

a. DAA accreditation decision is the official management authorization to operate the system(s). The accreditation grants approval for the system(s) to operate in a particular security mode, with a prescribed set of INFOSEC countermeasures. DAA signature required.

b. Potential List of enclosures (as required, or specified by DAA) include the following: Copies of MOAs, test results, ST&E, Contingency Plan, C&A Plan, Security Policy, Security Features Users Guide, Trusted Facility Manual, Security Continuity of Operations (CONOPS), Security Architecture, Covert Channel Analysis, and other documentation to support the accreditation.

BUPERS LAN EXTERNAL COMMUNICATIONS ACCESS REQUEST

Date of Request:	Pers-Code:	Phone:	Room:
User Name:		User ID:	Network Operating System:

SERVICE REQUIRED (Check all that apply)

☐ Dial-In (Home)

Home Operating system (version) _____ (Windows 95 is necessary for those using MS Exchange at BUPERS)

☐ Dial-In (Travel)

Date of Departure: _____

Date of Return: _____

☐ Dial out

System Name _____

System Phone _____

System POC _____

POC Phone _____

☐ INTERNET ☐ FTP ☐ WWW

PURPOSE/JUSTIFICATION:

I am advised that the unauthorized disclosure, retention, or negligent handling of LAN systems or information, or providing the means for unauthorized users to gain access by me could result in disciplinary action. I will report all violations or suspected misuse to the ISSO. I understand that according to the Fair Labor Standards Act, I am:

☐ Exempt, and may not be compensated for my time spent on work approved by this form.

☐ Non-Exempt, and must be compensated for my time spent on work approved by this form.

I understand that I may not put classified records on a computer that I use at work, home or at any other off-site location. I also understand that Privacy Act or other sensitive data (such as Navy budgetary, manpower, etc.) must be protected. I will ensure that other residents and guests of my household will not have access to Government records. I understand the access to the Internet is only for official purposes. I understand that copying software for personal use may be a violation of the United States copyright laws and that I may be personally liable for such illegal reproductions.

NAVPERS 5239/3 (Rev 2/98)

I understand this use of a personally-owned computer to do government work regardless of location is a privilege and can be revoked for non-compliance at any time or when the need no longer exists. Upon completion of said government work, all hardware will be returned, and government software and data completely removed from personally-owned equipment. I understand that if I am on travel, I must visit the LMC (room 2522) 1-2 days prior to travel to receive travel user ID and password.			
User Signature:			
I certify that user access is for official government business only			
Supervisor Signature:		Department Head Signature:	
Date of Activation:	Date of Termination:	ISSO Signature:	Date:
BUPERS NSO Signature:		Date:	
COMMENTS:			
FOR LAN MANAGEMENT CENTER USE ONLY			
Login ID:	Password Set: ☐ Yes ☐ No	Software Name:	
Assigned IP Address:	USER ID:	Password Set: ☐ Yes ☐ No	
Software Loaded: ☐ Yes ☐ No	Date Request Received:	Date of Activation:	Date of Termination:
COMMENTS:			
LMC Staff Signature:			

NAVPERS 5239/3 (Rev 2/98)

INFOSEC TRAINING OUTLINE

AIS SECURITY PERSONNEL

1. END USERS
2. TOP MANAGEMENT
3. SECURITY STAFF
4. ST&E TEAM
5. AUDIT TEAM
6. IG TEAM
7. PROCUREMENT

SUBJECT AREAS

1. GENERAL SECURITY AWARENESS (1 - 7)

    a. Threats to and Vulnerabilities of Computer Systems
    b. Use of Improved Computer Security Practices
    c. Specific Computer Security Policies and Procedures

2. SECURITY PROGRAM PLANNING/MANAGEMENT (1 - 7)

    a. Security Program Organization
    b. Security Planning
    c. Training Planning
    d. Audit and Monitoring
    e. Risk Analysis

3. COMPUTER SECURITY POLICIES AND PROCEDURES (1 - 7)

    a. Organizing the Security Responsibilities
    b. Security Implementation Plans
    c. Security Work Flow Control
    d. Personnel Practices and Responsibilities

4. CHANGE CONTROL AND COMPUTER ABUSE (1 - 6)

    a. Facility
    b. Hardware
    c. Software
    d. Telecommunications
    e. Data
    f. Human Resources
    g. Software Security Documentation

h. Documenting Computer Abuse Violations
i. Reporting Computer Abuse Violations

5. SOFTWARE SECURITY (3 - 6)

a. Operating System
b. Application System
c. Utility Routines

(1) Access Control and Authorization
(2) Detecting Attempted Violations
(3) Additional Software Functions
(4) Real Time Software Auditing
(5) Software Configuration Management

6. TELECOMMUNICATION SECURITY (3 - 6)

a. Dial Up
b. Point to Point
c. Network
d. Encryption
e. Fiber optics

7. TERMINAL/DEVICE SECURITY (3 - 6)

a. Access to Terminals and Output
b. Access to Computers and Files
c. Access to Communication Lines
d. Terminal Protection
e. Terminal Identification

8. SYSTEMS DESIGN SECURITY (3 - 6)

a. Project Initialization
b. Investigative Study
c. Generalized System Design
d. Detailed System Design
e. File Access Processing
f. Implementation Planning
g. Systems Implementation
h. Post Implementation Evaluation

9. HARDWARE SECURITY (3 - 6)

    a. Firmware
    b. Emanation Protection
    c. Encryption Devices
    d. COMSEC

10. PHYSICAL SECURITY (3 - 6)

    a. Building Design/Protection
    b. Emanation Protection
    c. Electric Power
    d. Fire Protection
    e. Air Conditioning
    f. Floods
    g. Earthquake
    h. Windstorm
    i. Housekeeping
    j. Alternative/Emergency Backup Facilities
    k. Access

11. PERSONNEL SECURITY (1 - 6)

    a. Personnel Selection Hiring Procedures
    b. Personnel Control
    c. Job Rotation Program
    d. Security Awareness Training Program
    e. Polygraph/Honesty Tests
    f. Background Investigations
    g. Access/Clearances
    h. Screening Techniques
    i. Security Briefing
    j. Disciplinary Actions
    k. Substance Abuse

12. AUDIT (2 - 5)

    a. Navy Management Policies for Conducting Audits
    b. Audit Trails in AISs
    c. Audit Controls in AISs
    d. Efficiency and Economy of Audit
    e. Legal Requirements for Navy Audit

f. Audit Tools and Techniques
g. Documentation of Audits
h. Procedures for Conducting an AIS Audit

13. DATA SECURITY (1, 3 - 6)

a. Unclassified
b. Sensitive Unclassified
c. Classified
d. Sensitive Compartmented Information (SCI)
e. Single Integrated Operational Plan-Extremely Sensitive Information (SIOP-ESI)
f. National Cryptographic Information

14. RISK ANALYSIS (2 - 5)

a. Data Collection

(1) Asset Identification
(2) Threat and Vulnerability Identification

b. Analysis

(1) Asset Valuation
(2) Threat and Vulnerability Evaluation
(3) Annual Loss Expectancy Analysis
(4) Cost Benefit Analysis of Countermeasure Alternatives
(5) Selection of Cost Effective Countermeasures

c. Documentation. Risk Analysis Documentation

15. CONTINGENCY/BACKUP PLANNING (1 - 4, 7)

a. Preliminary Planning

(1) Purpose
(2) Scope
(3) Assumptions
(4) Responsibilities
(5) Strategy

b. Preparatory Actions

(1) Personnel
(2) Data
(3) Software
(4) Hardware
(5) Communications
(6) Supplies
(7) Transportation
(8) Space
(9) Power and Environmental Controls
(10) Documentation
(11) Budget Requirements

c. Action Plan

(1) Emergency Response
(2) Backup Operations
(3) Recovery Actions
(4) Backup Site Agreement
(5) Annual Test Plan/Results

16. DISASTER RECOVERY (1 - 3)

a. Disaster Planning

(1) Emergency Phase
(2) Backup Phase
(3) Restoration Phase

b. Recovery Test and Evaluation

c. Recovery Operation Centers

17. SECURITY ACCREDITATION (1 - 5)

a. Categories of Data
b. Accreditation Authority
c. Accreditation Process
d. Accreditation Review
e. Accreditation Documentation Requirements

18. SECURITY TEST AND EVALUATION (ST&E) (1 - 4)

a. ST&E Requirement
b. ST&E Team Composition

c. ST&E Plan Development
d. Specific Test Requirements
e. Formal ST&E Test
f. Evaluation of Results and Recommendations

g. Documentation

19. AIS SECURITY AND NAVY CONTRACTOR INTERFACE (2, 3, 6)

a. Requirements for AIS Security
b. Industrial Security Regulation(s)
c. Navy Security Regulation
d. Other Government Agency Regulations
e. Software Configuration Control(s)
f. Contractor Accreditation Process
g. Accreditation Documentation

INFORMATION SYSTEMS SECURITY (INFOSEC) WARNING SCREEN

USE OF THIS OR ANY OTHER DOD COMPUTER SYSTEM
CONSTITUTES CONSENT TO MONITORING AT ALL TIMES

This is a Department of Defense (DOD) computer system. These computer systems, including all related equipment, networks, and network devices (specifically including Internet access), are provided only for authorized U.S. government use. DOD computer systems may be monitored for all lawful purposes, including ensuring that their use is authorized; for management of the system; to facilitate protection against unauthorized access; and to verify security procedures, survivability, and operational security. Monitoring includes active attacks by authorized DOD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied, and used for authorized purposes. All information, including personal information, placed on or sent over this system may be monitored. Use of this DOD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or adverse action. Use of this system constitutes consent to monitoring for these purposes.

BUPERS AIS SECURITY INCIDENT REPORT

From: ISSO (Org Code)

To: Information Systems Security Manager (Pers-0143)

Via: Branch/Division Head

1. Report date | Incident date

- ☐ Waste, Fraud, Abuse
- ☐ Theft
- ☐ Physical Destruction
- ☐ Data Modification
- ☐ Other
- ☐ Unauthorized Disclosure
- ☐ Unauthorized Use of User ID
- ☐ Password Violation
- ☐ Virus
- ☐ Network Infraction

2. Name, Rank/Grade, Code of Individuals Involved:

3. Approximate Cost of this Incident (downtime, replacement, labor):

4. Summary of Incident and Investigation Results:

5. Branch/Division Head Recommendations/Comments:

6. Name, Rank/Grade, Title of Investigating Official:

7. Recommended Action to Prevent Reoccurrence:

8. Recommended Action by BUPERS ISSM:

NAVPERS 5239/1 (Rev 2/98)

PERSNET LAN ACCOUNT REQUEST (PLAR)		
Section I. User Information/Request		
To: PERSNET Help Desk, Building 768 Via: (1) Supervisor (2) ISSO Subj: REQUEST FOR PERSNET LAN ACCOUNT		Date:
USER NAME (Last, First Middle)	Rank/Civilian/Contractor:	Phone Number:
Building Number:	Room/Cubicle Number:	User ID:
Request Action: ☐ Add ☐ Delete ☐ Modify ☐ Other		
Access Required: ☐ PERSNET ☐ E-MAIL	AIS Equipment Required: ☐ PC at Desk ☐ PC Required	
User Signature:		
Section II. Supervisor Approval		
Signature:		Date:
Section III. ISSO Approval		
Signature:		Date:
ISSO COMMENTS:		
SECTION IV. TO BE COMPLETED BY NCC PERSONNEL		
Account Number:	Created By:	Date:

NAVPERS 5239/4 (Rev 4-99)

USER RESPONSIBILITY AGREEMENT

As a PERSNET local or remote user, I am responsible and accountable for the following requirements of this agreement. I am solely responsible for all access and actions carried out under my user identification and password. As part of my responsibilities, I agree that I:

Will not disclose my password to anyone, nor will I write my password down.

Will not give my password to anyone else due to reassignment, transfer or termination.

Will limit the use of the PERSNET LAN to official government business.

Will not use computer resources for personal gain.

Will adhere to INTERNET policies and procedures.

Will notify ISSO/NSO immediately of computer security incidents.

Will not circumvent security requirements to obtain unauthorized access.

Will adhere to all security policies and rules concerning external connectivity.

Will report any changes in my status to the ISSO/NSO.

Will safeguard laptop (if issued to me) at all times. While in travel status, I will not leave laptop unsecured.

Will not change the configuration of any network component, including desktop/laptop computers.

Will not introduce software or hardware into the PERSNET infrastructure.

WARNING

USE OF ANY DoD INTEREST COMPUTER SYSTEM CONSTITUTES A CONSENT TO MONITORING AT ALL TIMES. PERSNET is a Department of Defense computer system. This computer system, including all related equipment, networks and network devices (specifically including INTERNET access), are provided only for authorized U.S. Government use. DoD computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability and operational security. Monitoring includes active attacks by authorized DoD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed on or sent over this system may be monitored. Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal or adverse action. Use of this system constitutes consent to monitoring for these purposes. **I UNDERSTAND THAT THE STAFF HAS THE RIGHT TO REVOKE MY ACCESS AND INSPECT ALL FILES WHICH I CREATE. FAILURE TO ADHERE TO THESE RULES WILL RESULT IN IMMEDIATE SUSPENSION OF YOUR ACCOUNT.**

USER NAME:	USER SIGNATURE:	DATE:

NAVPERS 5239/4 (Rev 4-99)

PERSONALLY-OWNED COMPUTER HARDWARE/SOFTWARE
USER AGREEMENT (HARDWARE INCLUDES PERSONAL DIGITAL ASSISTANT (PDA),
LAPTOP PERSONAL COMPUTER, PALM PILOTS, AND ANY OTHER
PERSONALLY OWNED HARDWARE/SOFTWARE)

NAME:	CODE:	PHONE NO:	BLDG NO:	ROOM NO:

COMPUTER MAKE:	MODEL:	SERIAL NO:
OPERATING SYSTEM:		

RULES AND RESPONSIBILITIES FOR NON-GOVERNMENT PERSONALLY OWNED COMPUTER AND SOFTWARE USED FOR PROCESSING GOVERNMENT DATA

No Classified data is handled, processed, or stored on personally owned computer.

Copyright and license agreements must not be violated.

Government is relieved of any liability for personally owned computer hardware/software.

Government computer technician will perform installation/configuration of personally owned hardware to interface with Government system.

All application programs developed to manipulate or process Government business, financial, property, or Personal data on this personally owned computer are Government property.

I the owner certify with my signature below that all Government property and data will be removed and the PDA sanitized prior to permanent removal from the command.

Why is personally owned computer hardware/software being used?

_____

The undersigned accepts the above responsibilities to use their personally owned hardware/software for Government use.

OWNER SIGNATURE:	DATE:

DEPARTMENT DIRECTOR

☐ APPROVED ☐ DISAPPROVED	SIGNATURE:	DATE:

ISSO/ISSM

☐ APPROVED ☐ DISAPPROVED	SIGNATURE:	DATE:

CERTIFICATION – SANITIZATION OF PERSONALLY OWNED PDA

I _____ **, certify that all Government property and data has been removed and the PDA listed above has been sanitized prior to removal from the command.**

OWNER SIGNATURE:	DATE:

NAVPERS 5239/5 (Rev. 12-00)

SECRET SIPRNET LAN
ACCOUNT REQUEST

From: BUPERS/NAVPERSCOM ISSM (PERS-0143)
To: NAVPERSCOM Millington Helpdesk, Building 768

Subj: REQUEST FOR SECRET SIPRNET LAN ACCOUNT

Ref: (a) SECNAVINST 5510.36
(b) SECNAVINST 5510.30A
(c) SECNAVINST 5239.3
(d) OPNAVINST 5239.1A
(e) BUPERSINST 5239.1A

Personal Information			
Name: (Last, First, MI) *Print*			Rank/Civilian/Contractor
Phone	Building	Room	User ID

Requested Action

☐ **Add** ☐ **Delete** ☐ **Modify (permission)**

Access Required

☐ **SIPRNET (classified)** ☐ **E-mail**

ISSM Comments

Supervisor/ Director		Date

Secret Clearance Verification		Date
BUPERS ISSM		Date

To Be Completed By NCC Personnel

Account Name	Created By	Date

SECRET SIPRNET LAN
ACCOUNT REQUEST

NAVPERS 5239/6 (01/01)

As a user of the SIPRNET (classified) ADP systems I understand that…

I am responsible and accountable for following all requirements of references (a) through (e). I am solely responsible for all access and actions carried out under my user identification/password. As part of my responsibilities, I agree to the following conditions:

a. The requirements for access to classified information per references (a) and (b) will **be met.**

b. The password will **be kept secret and** will not **be disclosed to anyone,** will not **be electronically stored,** will not **be written down, and** will **be committed to memory.**

c. The SIPRNET password and User Account identification will not **be transferred to anyone else due to reassignment or transfer or termination.**

d. Use of SIPRNET will **be limited to official government business.**

e. Computer fraud will not **be committed. This includes but is not limited to:**

(1) Unauthorized input of false records or data into the system.

(2) Unauthorized use of computer facilities (i.e., theft of computer time), including use of a user name or password other than one's own.

(3) Unauthorized alteration or destruction of information, files or equipment.

(4) Introduction of unauthorized systems/software into the SIPRNET.

(5) Introduction of viruses, worms or any other destructive program into the SIPRNET.

f. Information Systems Security Manager (ISSM) will **be immediately notified of suspected cases of computer fraud.**

g. If the password is compromised, whether suspected, or confirmed, the compromise will **be immediately reported to the ISSM and the password** will **be immediately changed.**

h. Classified data will not **be entered, displayed, or processed where visible to unauthorized personnel.**

i. Security requirements will not **be circumvented in order to obtain unauthorized access.**

j. ISSM will **be notified in writing when access to the SIPRNET is no longer required due to reassignment, transfer, or termination.**

k. All classified media (paper, disks, CD-ROM) will **be handled and safeguarded per reference (a).**

l. All data hardcopy outputs and media will **be labeled to the highest level of data contained within.**

g. Cipher lock combinations and Electronic Badging Access Control System (EBACS) badges will not **be given to anyone.**

h. The SIPRNET terminal will not **be vacated while in operation. When leaving the SIPRNET Terminal area, ensure the area is clear of all classified information, terminal shutdown, and door securely locked.**

I certify that the above information is correct to the best of my knowledge and I will comply with the terms of this agreement. I certify that the security requirements identified in references (a) and (b) will be followed and that my security clearance and access is correct. I agree to notify NAVPERSCOM (PERS-341) and ISSM immediately of any action taken to revoke or downgrade my security clearance.

USER NAME (PRINT)	**DATE**
User Signature	

NAVPERS 5239/6 (01/01)